

Computing the generator polynomials of $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes

Joaquim Borges Ayats,^{1,2} Cristina Fernández-Córdoba,^{1,2}
Roger Ten-Valls^{1,2}

*Department of Information and Communications Engineering
Universitat Autònoma de Barcelona
Bellaterra, Spain*

Abstract

A $\mathbb{Z}_2\mathbb{Z}_4$ -additive code $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is called cyclic if the set of coordinates can be partitioned into two subsets, the set of \mathbb{Z}_2 and the set of \mathbb{Z}_4 coordinates, such that any simultaneous cyclic shift of the coordinates of both subsets leaves invariant the code. These codes can be identified as submodules of the $\mathbb{Z}_4[x]$ -module $\mathbb{Z}_2[x]/(x^\alpha - 1) \times \mathbb{Z}_4[x]/(x^\beta - 1)$. Any $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic code \mathcal{C} is of the form $\langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x)) \rangle$ for some $b(x), \ell(x) \in \mathbb{Z}_2[x]/(x^\alpha - 1)$ and $f(x), h(x) \in \mathbb{Z}_4[x]/(x^\beta - 1)$. A new algorithm is presented to compute the generator polynomials for $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes.

Keywords: Generator polynomials, MAGMA package, $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes.

¹ This work has been partially supported by the Spanish MINECO grant TIN2013-40524-P and by the Catalan AGAUR grant 2014SGR-691.

² Email: {joaquim.borges, cristina.fernandez, roger.ten}@uab.cat

1 Introduction

Denote by \mathbb{Z}_2 and \mathbb{Z}_4 the rings of integers modulo 2 and modulo 4, respectively. We denote the space of n -tuples over these rings as \mathbb{Z}_2^n and \mathbb{Z}_4^n . A binary code is any non-empty subset C of \mathbb{Z}_2^n . If that subset is a vector space, then we say that it is a linear code. Any non-empty subset \mathcal{C} of \mathbb{Z}_4^n is a quaternary code and a submodule of \mathbb{Z}_4^n is called a quaternary linear code. As general references on binary and quaternary codes, see [7],[8] and [9].

In Delsarte's 1973 paper (see [6]), he defined additive codes as subgroups of the underlying abelian group in a translation association scheme. For the binary Hamming scheme, namely, when the underlying abelian group is of order 2^n , the only structures for the abelian group are those of the form $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, with $\alpha + 2\beta = n$. This means that the subgroups \mathcal{C} of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ are the only additive codes in a binary Hamming scheme. In [2], $\mathbb{Z}_2\mathbb{Z}_4$ -additive codes were studied.

For vectors $\mathbf{u} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ we write $\mathbf{u} = (u \mid u')$ where $u = (u_0, \dots, u_{\alpha-1}) \in \mathbb{Z}_2^\alpha$ and $u' = (u'_0, \dots, u'_{\beta-1}) \in \mathbb{Z}_4^\beta$.

Let \mathcal{C} be a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code. Since \mathcal{C} is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, it is also isomorphic to a commutative structure like $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, \mathcal{C} is of type $2^\gamma 4^\delta$ as a group, it has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords and the number of order two codewords in \mathcal{C} is $2^{\gamma+\delta}$.

Let X (respectively Y) be the set of \mathbb{Z}_2 (respectively \mathbb{Z}_4) coordinate positions, so $|X| = \alpha$ and $|Y| = \beta$. Unless otherwise stated, the set X corresponds to the first α coordinates and Y corresponds to the last β coordinates. Call \mathcal{C}_X (respectively \mathcal{C}_Y) the punctured code of \mathcal{C} by deleting the coordinates outside X (respectively Y). Let \mathcal{C}_b be the subcode of \mathcal{C} which contains all order two codewords and let κ be the dimension of $(\mathcal{C}_b)_X$, which is a binary linear code. For the case $\alpha = 0$, we will write $\kappa = 0$.

Considering all these parameters, we will say that \mathcal{C} is of type $(\alpha, \beta; \gamma, \delta; \kappa)$. Notice that \mathcal{C}_Y is a quaternary linear code of type $(0, \beta; \gamma_Y, \delta; 0)$, where $0 \leq \gamma_Y \leq \gamma$, and \mathcal{C}_X is a binary linear code of type $(\alpha, 0; \gamma_X, 0; \gamma_X)$, where $\kappa \leq \gamma_X \leq \kappa + \delta$.

In [2], it is shown that a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code is permutation equivalent to a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code with standard generator matrix of the form

$$\mathcal{G} = (\mathcal{G}_X \mid \mathcal{G}_Y) = \left(\begin{array}{cc|ccc} I_\kappa & T_b & 2T_2 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 2T_1 & 2I_{\gamma-\kappa} & \mathbf{0} \\ \hline \mathbf{0} & S_b & S_q & R & I_\delta \end{array} \right), \quad (1)$$

where I_k is the identity matrix of size $k \times k$; T_b, S_b are matrices over \mathbb{Z}_2 ; T_1, T_2, R are matrices over \mathbb{Z}_4 with all entries in $\{0, 1\} \subset \mathbb{Z}_4$; and S_q is a matrix over \mathbb{Z}_4 .

The aim of this paper is to present an algorithmic method to compute the generator polynomials of $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes. The paper is organized as follows. In Section 2, we will introduce $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes and we will give a description of their generator polynomials. In Section 3, we will explain the algorithm to compute the generator polynomials of a given $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic code. This algorithm has been implemented and forms part of a package developed in MAGMA within the *Combinatorics, Coding and Security Group* from Universitat Autònoma de Barcelona (CCSG, <http://ccsg.uab.cat/>)[3], [5]. Finally, in Section 4, we will give some conclusions about our work.

2 $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes

Let $\mathbf{u} = (u \mid u') \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ and i be an integer. Then we denote by

$$\mathbf{u}^{(i)} = (u^{(i)} \mid u'^{(i)}) = (u_{0+i}, u_{1+i}, \dots, u_{\alpha-1+i} \mid u'_{0+i}, u'_{1+i}, \dots, u'_{\beta-1+i})$$

the cyclic i th shift of \mathbf{u} , where the subscripts are read modulo α and β , respectively.

We say that a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is *cyclic* if for any codeword $\mathbf{u} \in \mathcal{C}$, we have $\mathbf{u}^{(1)} \in \mathcal{C}$. $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes have been studied in [1] and [4].

Let $R_{\alpha,\beta} = \mathbb{Z}_2[x]/(x^\alpha - 1) \times \mathbb{Z}_4[x]/(x^\beta - 1)$, for $\beta \geq 0$ odd. We define the bijective map $\theta : \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \longrightarrow R_{\alpha,\beta}$ such that

$$\theta(v_0, \dots, v_{\alpha-1} \mid v'_0, \dots, v'_{\beta-1}) = (v_0 + v_1x + \dots + v_{\alpha-1}x^{\alpha-1} \mid v'_0 + v'_1x + \dots + v'_{\beta-1}x^{\beta-1}).$$

It is known that $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes are identified as $\mathbb{Z}_4[x]$ -submodules of $R_{\alpha,\beta}$ via θ , [1]. Moreover, if \mathcal{C} is a $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ with β odd, then there exist polynomials $b(x), \ell(x) \in \mathbb{Z}_2[x]$, and polynomials $f(x), h(x) \in \mathbb{Z}_4[x]$ such that satisfy the following conditions:

- (C1) $f(x)$ and $h(x)$ are coprime divisors of $x^\beta - 1$,
- (C2) $b(x)$ divides $x^\alpha - 1$,
- (C3) $\deg(\ell(x)) < \deg(b(x))$,
- (C4) $b(x)$ divides $\frac{x^\beta - 1}{f(x)}\ell(x) \pmod{2}$,

and

$$\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x)) \rangle.$$

3 Computing the generator polynomials

Let \mathcal{D} be a quaternary linear code of length β . Define the *torsion* code of \mathcal{D} as $Tor(\mathcal{D}) = \{v \in \{0, 1\}^\beta \mid 2v \in \mathcal{D}\}$. Define also the *residue* code of \mathcal{D} as $Res(\mathcal{D}) = \{\mu(z) \mid z \in \mathcal{D}\}$, where $\mu(x) = \mu(z_1 \dots, z_\beta) = (\mu(z_1), \dots, \mu(z_\beta))$ is the modulo 2 map from \mathbb{Z}_4 to \mathbb{Z}_2 . Note that $Tor(\mathcal{D})$ and $Res(\mathcal{D})$ are binary linear codes. Moreover, if \mathcal{D} is cyclic, then so are $Tor(\mathcal{D})$ and $Res(\mathcal{D})$.

The following algorithm computes the generator polynomials for a $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic code.

Algorithm 1 *Input: A $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic code, \mathcal{C} of type $(\alpha, \beta; \gamma, \delta; \kappa)$ with β odd and generator matrix $\mathcal{G} = (\mathcal{G}_X \mid \mathcal{G}_Y)$.*

Step 1: Calculate the generator polynomial $\bar{f}(x)$ of the binary code $Tor(\mathcal{C}_Y)$.

Step 2: Calculate the generator polynomial $\bar{f}(x)\bar{h}(x)$ of the binary code $Res(\mathcal{C}_Y)$.

Step 3: Compute $f(x)$ and $h(x)$ the Hensel lift of $\bar{f}(x)$ and $\bar{h}(x)$, respectively.

Step 4: Calculate the generator polynomial $b(x)$ of the code $\mathcal{C}_0 = \{w \in \mathbb{Z}_2^\alpha \mid (w \mid 0, \dots, 0) \in \mathcal{C}\}$.

Step 5: Find $\mathbf{v} \in \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ such that $\mathbf{v}\mathcal{G}_Y = \theta^{-1}(f(x)h(x) + 2f(x))$.

Step 6: Compute the polynomial $\ell(x) = \theta(\mathbf{v}\mathcal{G}_X) \bmod (b(x))$.

Output: The generator polynomials $b(x), \ell(x), f(x)$ and $h(x)$.

Theorem 3.1 *Let \mathcal{C} be a $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ with β odd. The output polynomials $b(x), \ell(x), f(x)$ and $h(x)$ of Algorithm 1 verify Conditions (C1), (C2), (C3), (C4), and*

$$\mathcal{C} = \langle (b(x) \mid 0), (\ell(x) \mid f(x)h(x) + 2f(x)) \rangle.$$

4 Conclusion

In this paper, we have presented an algorithm to compute the generator polynomials of a $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic code. We are developing a package to work with $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes within the MAGMA environment. It is important to mention that MAGMA provides machinery to study cyclic codes over finite fields \mathbb{F}_q , over the integer residue classes \mathbb{Z}_m , and over Galois rings $GR(p^n, k)$. The ring \mathbb{Z}_4 receives a special attention and there are available

specific functions to work with codes over \mathbb{Z}_4 . Nevertheless, MAGMA provides functions to get the generator polynomials for cyclic codes only over finite fields, e.g., for binary cyclic codes.

A version of the package for $\mathbb{Z}_2\mathbb{Z}_4$ -additive codes developed by the *Combinatorics, Coding and Security Group* and the manual with the description of all functions can be downloaded from the *CCSG* web page <http://ccsg.uab.cat/>. The package provides a tool to work with codes over \mathbb{Z}_4 considering $\mathbb{Z}_2\mathbb{Z}_4$ -additive codes with $\alpha = 0$.

Given a cyclic code, \mathcal{C} , over \mathbb{Z}_4 of odd length, there exist generator polynomials $f(x)$ and $h(x)$ such that $\mathcal{C} = \langle f(x)h(x) + 2f(x) \rangle$, see [9, Theorem 7.26]. Our Algorithm 1 allows to compute the polynomials $f(x)$ and $h(x)$ when $\alpha = 0$ and β is odd.

The functionalities for $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes will be soon available in the new version of the *CCSG* package for $\mathbb{Z}_2\mathbb{Z}_4$ -additive codes. For any comment or further information, you can send an email to support-ccsg@deic.uab.cat.

Acknowledgement

The authors would like to thank Jaume Pujol and Mercè Villanueva for their reviews and comments in the development of the MAGMA package for $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes.

References

- [1] Abualrub, T., I. Siap and N. Aydin, *$\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes*, IEEE Trans. Info. Theory **60** (2014), 1508–1514.
- [2] Borges, J., C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva, *$\mathbb{Z}_2\mathbb{Z}_4$ -linear codes: generator matrices and duality*, Designs, Codes and Cryptography **54** (2010), 167–179.
- [3] Borges, J., C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva, “ $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes. A MAGMA package,” Universitat Autònoma de Barcelona, Version 3.4, 2012.
- [4] Borges, J., C. Fernández-Córdoba and R. Ten-Valls, *$\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes, generator polynomials and dual codes*, submitted. arXiv:1406.4425.
- [5] Bosma, W., J. J. Cannon, C. Fieker and A. Steel (Eds.), “Handbook of MAGMA functions,” Edition 2.16, 5017 pages, 2010.

- [6] Delsarte, P., *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. **10** (1973).
- [7] Huffman, W.C., and V. Pless, “Fundamentals of Error-Correcting Codes,” Cambridge University Press, Cambridge, 2003.
- [8] MacWilliams, F.J., and N.J.A. Sloane, “The Theory of Error-Correcting Codes,” North-Holland Publishing Company, Amsterdam, New York, Oxford, 1975.
- [9] Wan, Z., “Quaternary Codes,” World Scientific, Series on applied mathematics v. 8, 1997.